RSAC 2025 Conference

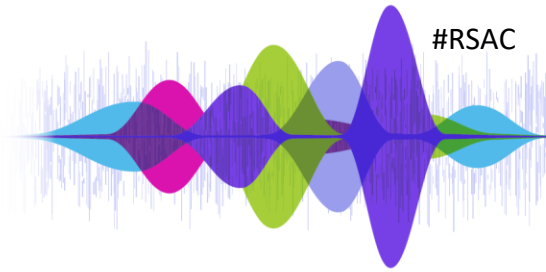
Many Voices.
One Community.

SESSION ID: DSA-M05

Space Assets Resiliency: Protecting Against Current Attack Techniques

H. Barbara Grofe
GICSP, CISSP-ISSAP-ISSEP-ISSMP, HCISPP, CSSLP, CISM, CGEIT, DoDD 8140, 8570 IAM_IAT I-II-III, IASAE I-II, CND-SP, CCSK, PCII, ITIL, MDQM

Space Asset Security Architect
Spartan Corp
https://www.linkedin.com/in/barbaragrofeitconsultant/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Slides 32, 33 and 34 and the technology presented are the property of Schneider Electric.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Introduction

Session objectives and scope

- Understanding evolving threats to space assets
- Exploring protection technologies
- Developing integrated resilience strategies

Current state of space asset vulnerability

- Over 28,000+ satellites in orbit, over 59,000 categorized since 1957.
- 73% increase in documented threat incidents over the last 3 years
- 89% of space asset operators report security as a primary concern

Security and Resiliency Implementation Challenges

Space Environment

- Vacuum
- Ultraviolet (UV) radiation
- Ionizing particle radiation (protons/ electrons)
- Extreme temperatures -55C to -125C (-67F to -193F)
- On-orbit charging (electrostatic discharge)
- Atomic Oxygen (AO) = O instead of O^2

Satellite

- Power limitations and needs
- Container space limitations
- Weight
- Vibration
- Cost

Impacts Engineering Decisions and Control Implementation

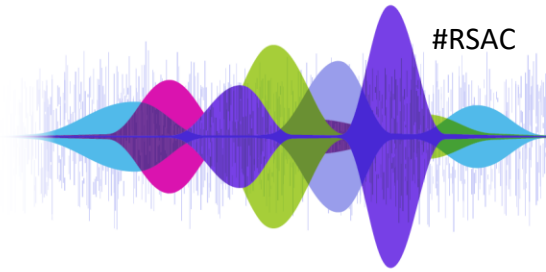
Current and Future Threat Environment

The environment is dangerous, and threats are increasing in velocity and sophistication.

These include:

- Directed energy weapon proliferation
- Sophisticated jamming and spoofing techniques
- Dazzling
- Cyber threats to satellites and ground control systems
- Physical threats such as Direct-Ascent Anti-Satellite Weapons (DA-ASAT)and co-orbital systems
- Environmental hazards such as space debris and solar events

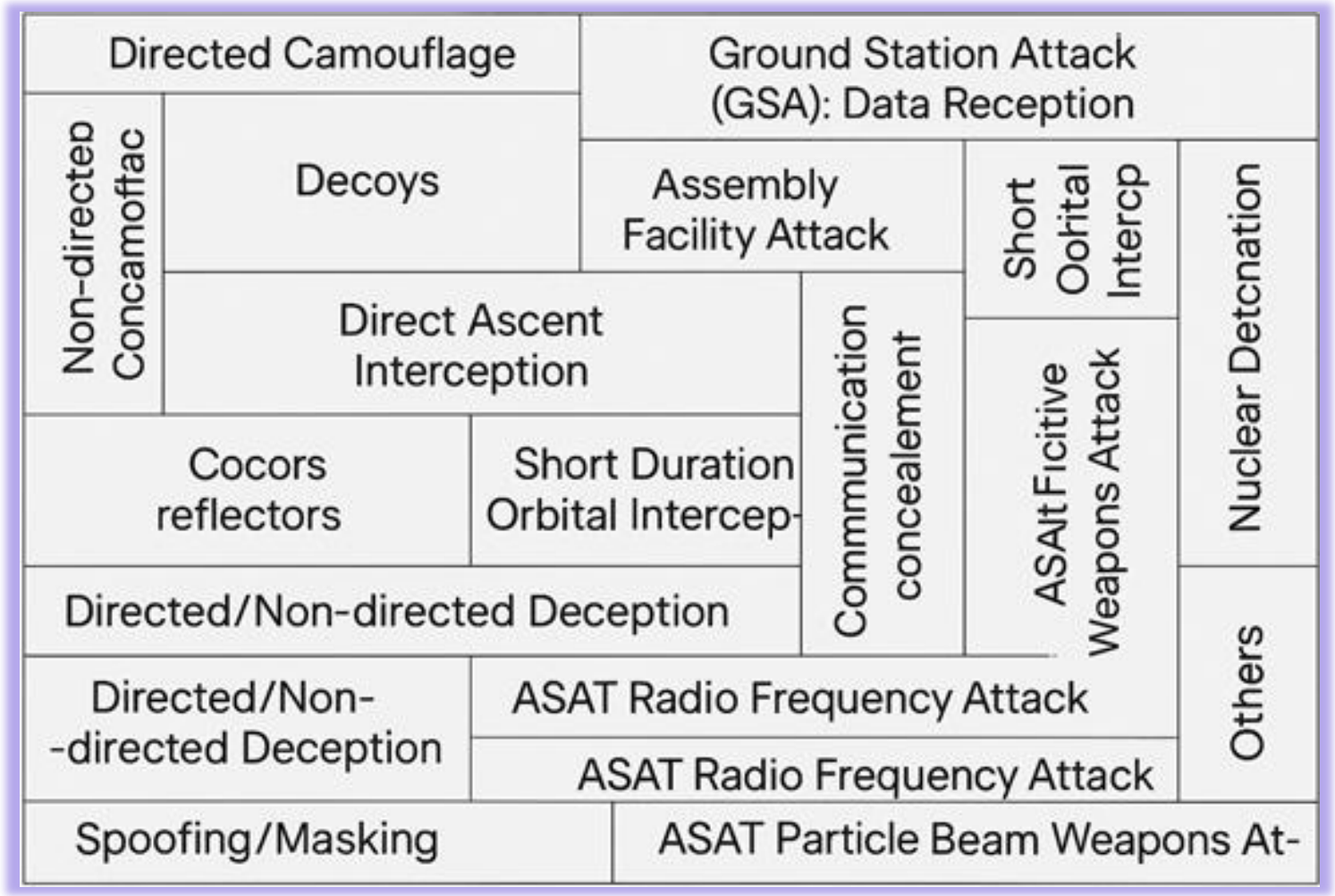
Theoretical to Demonstrated



Space Asset Assaults

- Starlink: Hacker created a hacking tool (modchip) attached to a Starlink dish that can launch a fault injection attack to bypass security protections, allowing the hacker to reach deeper into the system. (Ka and Ku band)
- U.S. intelligence analysts have confirmed that Russia executed a cyberattack on a targeted ground station that compromised Viasat's KA-SAT satellite broadband service and disrupted Ukraine's military communications in February 2022.
- In 2016, NASA's Deep Space Network (DSN), which is the communication infrastructure for deep space missions, was the command and control for the MARS rover. It was identified that there were hacking scripts and guides to exploit the MARS Rover on the Internet. Only in 2016 was this connection and network encrypted.
- In April 2022, at HackCYSAT in Paris, France. The following attacks were executed on an ESA satellite:
  - Integrity attack of imagery from the onboard camera
  - Through escalation of privileges, installed malicious code and executed that code
  - Ransomware attack on the satellite

Subset of Space Asset Attacks



Space Asset Resilience

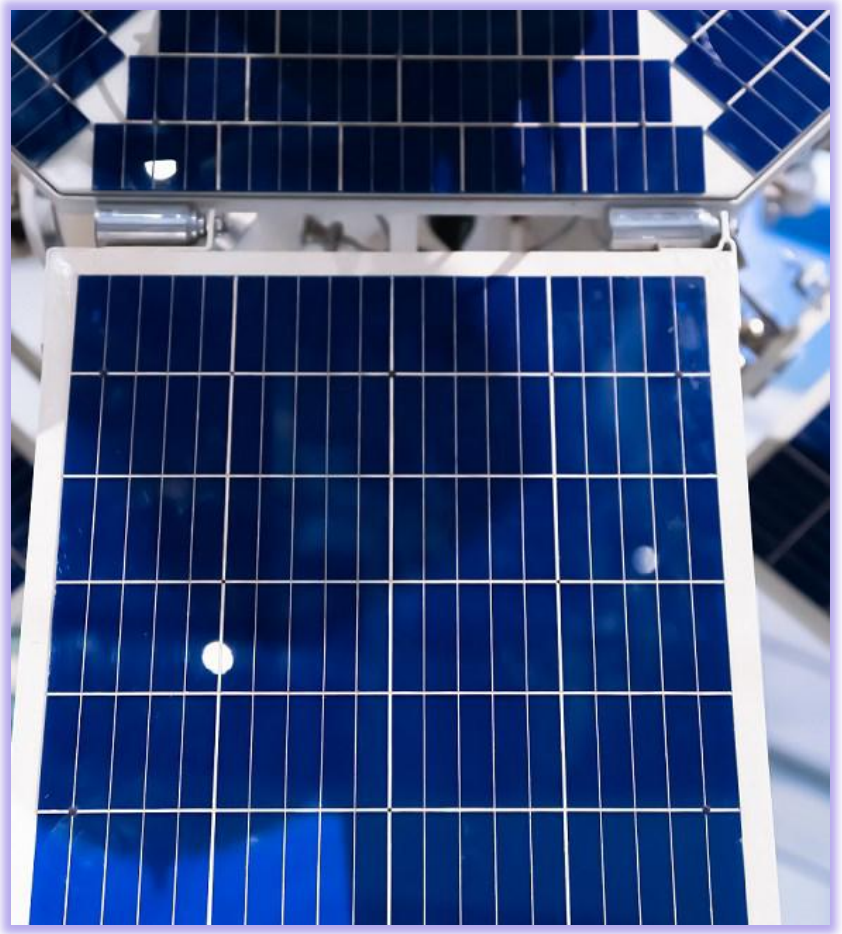
Why is resiliency important?

- Critical infrastructure dependency on space assets
- Our growing dependency on space for every business and technological sector
- Current conflicts and space-based battle theater dominance
- The expanding commercial space ecosystem

Space Assets are Critical Infrastructure

Important Subsystems of a Space Asset

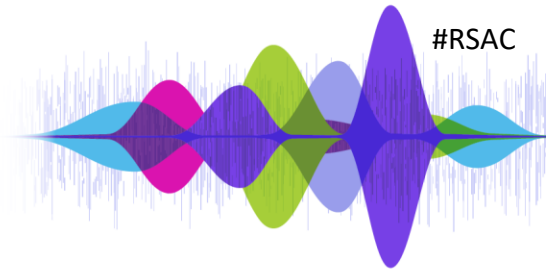
- Asset Bus and Network
- Propulsion Subsystems
- Attitude and Articulation Control Subsystems
- Power Supply/ Distribution Subsystems
- Communication Subsystem
- On-Board Computer
- Payload system
- Data Handling Subsystems
- Environmental Subsystems
- Landing Subsystems
- Launch Facilities
- Ground Stations/ Antenna



★ *Can be hacked*

RSAC 2025 Conference

Categories of Threats and Potential Mitigations



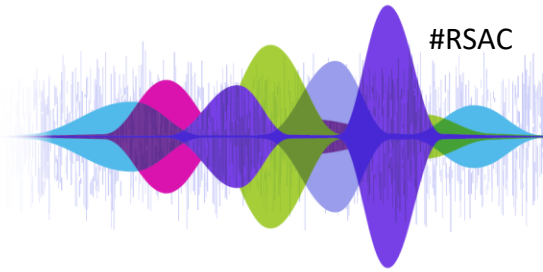
Threat: Directed Energy Weapon

Evolving military technology with significant implications for space-based assets that uses energy to disable and damage targets.

- High-Energy Lasers (HELs)
- High-Power Microwaves (HPMs)
- Particle Beams (Largely theoretical)

– Strategic Advantages of Directed Energy Weapons

- Speed
- Precision
- Scalable Effects
- Deniability



Mitigation: Directed Energy Weapon

- Distributed constellation designs to increase resilience
- Hardened optical sensors resistant to dazzling
- Maneuverability to avoid sustained targeting

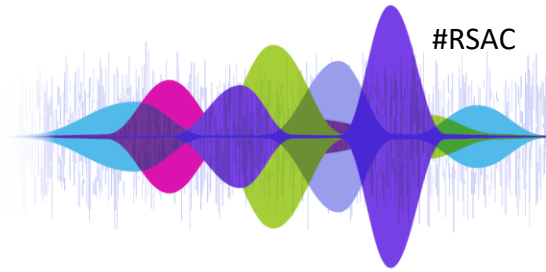
Additional protections in development next 2 – 3 years

- Reflective metamaterial surfaces with tunable properties show 70-85% effectiveness against specific laser wavelengths in laboratory conditions
- Sensor network for attack detection and characterization achieves 95% accuracy in ground testing

Threat: Electronic Warfare (EW)

Electronic Attack (EA)

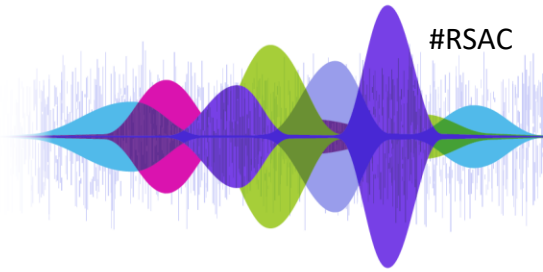
- Uplink Jamming: Disrupts signals sent from ground stations to satellites
- Downlink Jamming: Interferes with signals from satellites to ground receivers
- Spoofing: Transmits false signals that mimic legitimate ones, potentially providing false data or acquisition of control
- Meaconing: Intercepts, delays, and rebroadcasts legitimate signals to create confusion



Susceptibility

Space systems are particularly susceptible to electronic warfare due to:

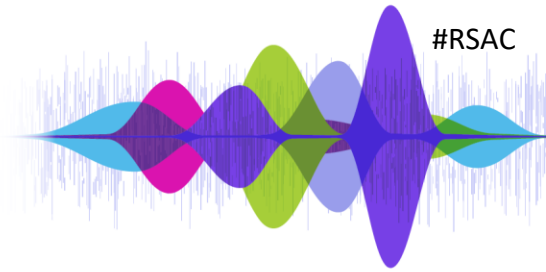
- Reliance on Electromagnetic Signals: Necessary for operation and communication.
- Distance: The vast distances make the signals susceptible to interference
- Power Limitations: Satellites have limited power making it easier for ground-based jammers with greater power resources to overwhelm them
- Predictable Orbits: Most satellites follow known paths, making them predictable targets
- Limited Shielding: Weight constraints limit the amount of electromagnetic shielding possible



Mitigation: Electronic Warfare (EW)

Electronic Protection (EP)

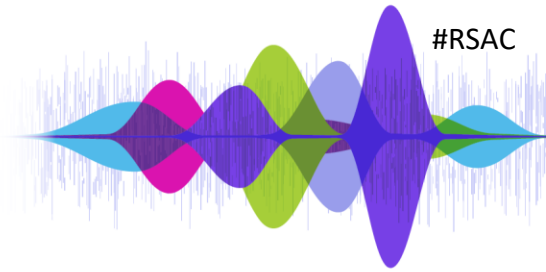
- Frequency Hopping: Rapidly switching frequencies to avoid sustained jamming
- Directional Antennas: Focusing signal strength and reducing vulnerability to jamming
- Encryption: Protecting commands and data from interception or manipulation
- Signal Processing: Filtering techniques to distinguish legitimate signals from interference



Threats: Physical Attacks

Direct-Ascent Anti-Satellite Weapons (DA-ASAT)

- Missile-Based Systems: Ground, sea, or air-launched missiles designed to intercept and destroy satellites
- Co-Orbital Anti-Satellite Systems
  - Rendezvous & Proximity Operations (RPO): Satellites that can approach other satellites
  - Killer Satellites: Spacecraft designed to damage others via collision, robotic arms, or other mechanisms
- Physical Ground Infrastructure Attacks
  - Targeting Ground Stations: Physical attacks against terrestrial control facilities
  - Launch Facility Strikes: Disabling the ability to launch, replace or repair space assets
  - Supply Chain Disruption: Targeting manufacturing or components manufacturers



Mitigations: Physical Attacks

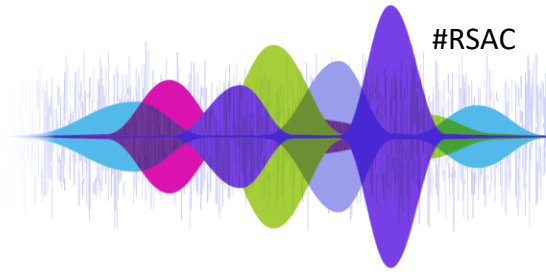
Defensive Countermeasures

- Space powers are developing various defensive approaches:
  - Maneuverability: Satellite propulsion systems that allow evasive actions
  - Distributed Architectures: Using constellation of smaller satellites
  - Rapid Reconstitution: The ability to quickly replace lost capabilities through responsive launch
  - Hardening: Physical reinforcement against impacts or explosions

Threats: Cyber Attacks and Exploits

Primary Attack Vectors

- Ground Segment Vulnerabilities
  - Command and Control Centers: Targeting the facilities that manage satellites
  - Data Downlink Stations: Compromising facilities that receive satellite data
  - Network Infrastructure: Exploiting connected systems to gain access to space control networks
- Communication/Transmission Link Exploitation
  - Man-in-the-Middle Attacks: Positioning between legitimate communications to manipulate data
  - Replay Attacks: Recording and retransmitting legitimate commands at a later time
- Onboard System Vulnerabilities
  - Malicious Code Injection: Uploading harmful commands or software during updates
  - Side-Channel Attacks: Using electromagnetic emissions to extract information

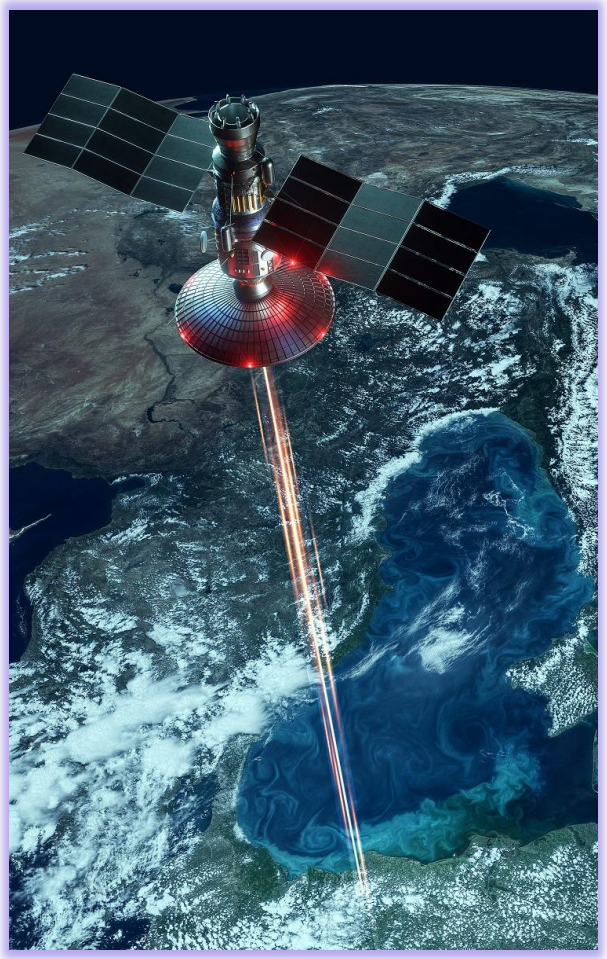


Threats: Cyber Attacks and Exploits

Strategic Impacts

- Cyber attacks on space assets can achieve several effects:
  - Loss of Control: Preventing legitimate operators from commanding their satellites
  - Data Theft: Stealing sensitive information collected by surveillance satellites
  - Service Denial: Disrupting services like GPS, communications, or weather forecasting
  - Permanent Damage: Manipulating systems to cause physical harm
- Several specific weaknesses make space systems particularly susceptible:
  - Legacy Systems: Most satellites use older technology without modern security features
  - Limited Resources: Constrained computing power restricts use of sophisticated security measures
  - Difficulty of Updates: Challenges in patching orbiting systems
  - Extended Operational Lifetimes: Satellites designed before current cyber threats emerged

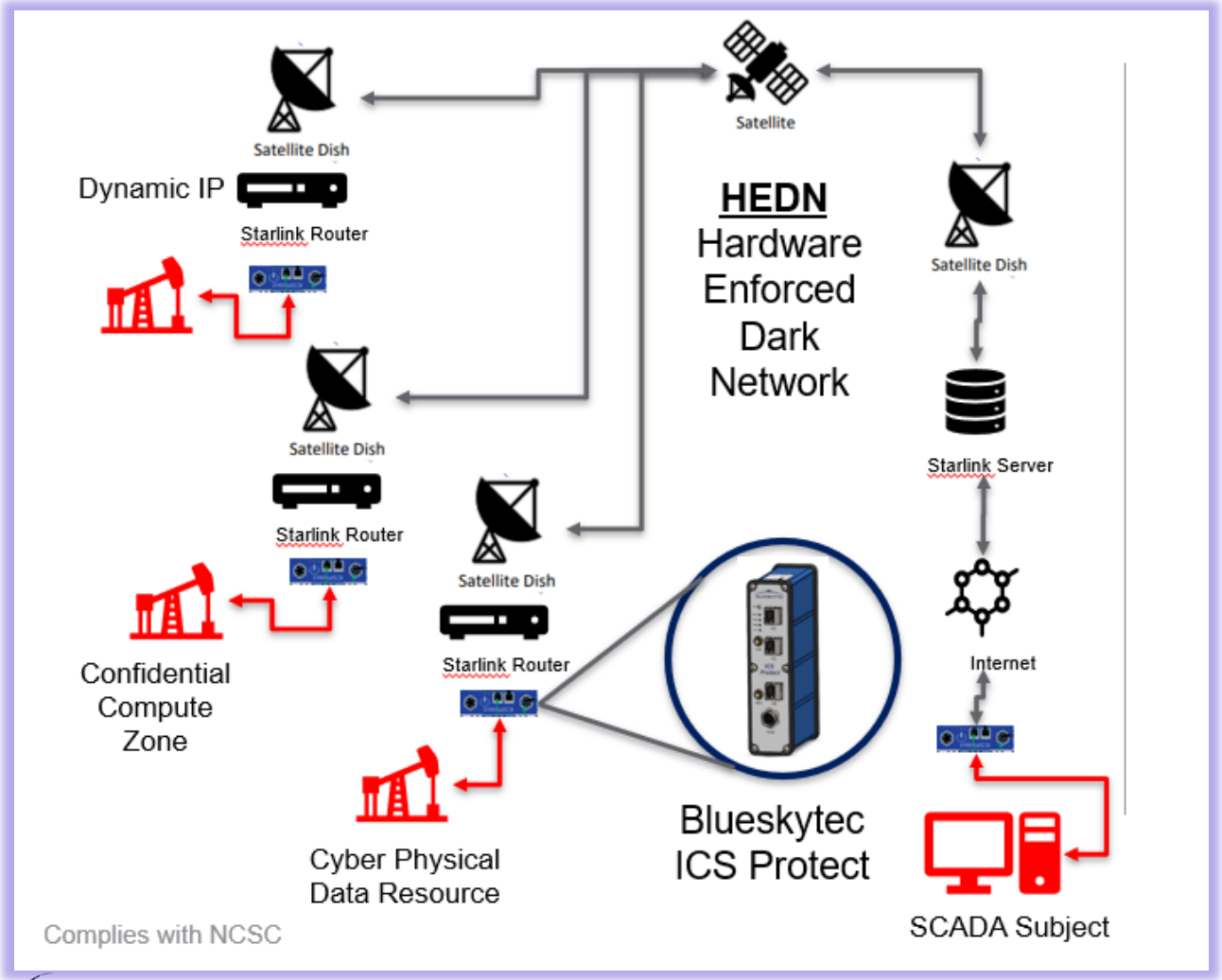
Mitigation: Cyber Attacks and Exploits



Defensive Approaches

- Encryption: Protecting command and data with strong cryptography
- Authentication Protocols: Verifying the source of commands
- Zero-Trust Architectures: Requiring verification for all system interactions
- Anomaly Detection: Monitoring for unusual behavior that might indicate compromise
- Segmentation: Isolating critical systems from other systems
- Validated Supply Chain: Ensuring authenticity and specifications of parts, assemblies, and components.
- Space Range: Testing environments for identifying vulnerabilities before launch

Hardware Security Field Programmable Gate Arrays (FPGA) for Cryptography



ENCRYTPTION – Quantum Immortality

Distributed One Time Pad Symmetric Key for every Data Transaction provides Post Quantum Cryptography (QPC) Immunity

SYSTEM – Fully Integrated

Automated FPGA Policy Decision End Points delivers Integrated Immutable Authentication, Firewall, Encryption, Data Flow, Alarm + Event Intelligence

BREACH – Threat Elimination

Defence by Denial Protection through the Kill Chain™ . Physical and Quantum Anti-Tamper, No IP to Ping for Targeting. Ingress & Egress IP Port/IP listing to block Callback. Limits Blast Radius to Compute Zone

FATIGUE – Mission Sovereignty

Software Bill of Materials (SBOM) Free, Distributed Keys For Life, No OS / Firmware updates. Bump in Wire deployment

Space Range Capabilities

Space Domain Awareness (SDA) module
- Platform Development
- Sensor Integration
- AI-Enabled Command and Control
- Data Processing and Analytics
- Interoperability and Integration
- Resilience and Sustainability

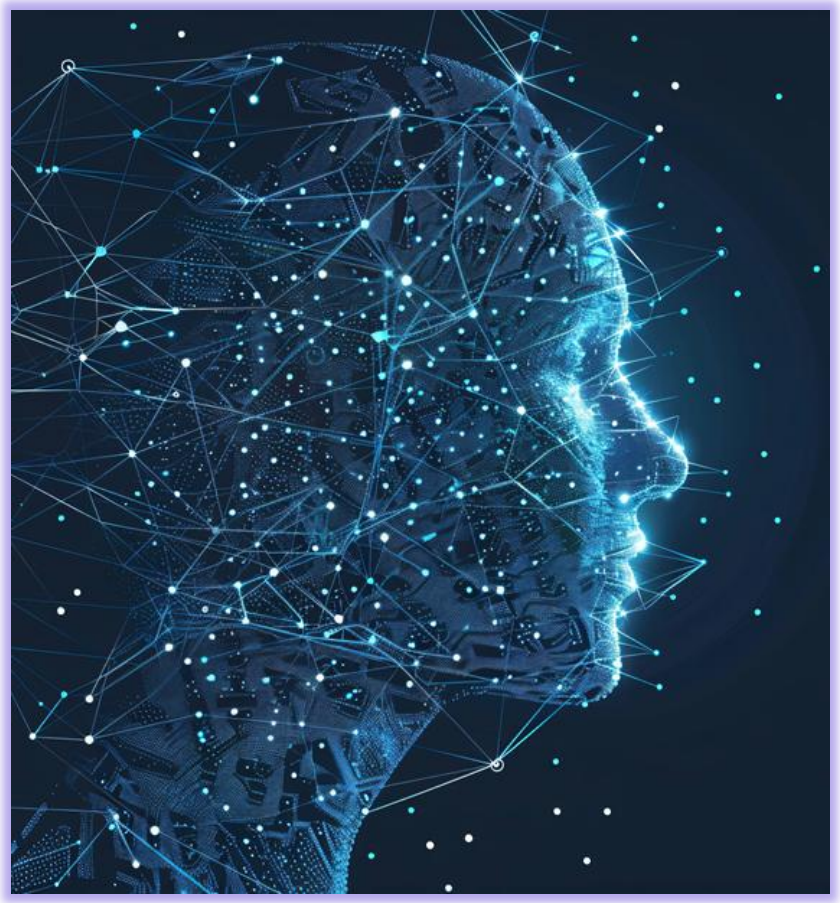
Space Systems Integration (SSI) module
- Advanced Space Connectivity and Integration
- Enhanced Space Systems and Capabilities
- Next-Generation Hardware and Security Measures
- Precision Positioning Technologies
- Radio Frequency Space Data Transport Solutions
- Automate on-orbit situational awareness

Satellite Resilience & Cybersecurity module (SRC)
- Vulnerability and Flow Management
- Secure Protocols and Methodologies
- Space-appropriate specifications
- Standards & Certification

RSAC 2025 Conference

New Technologies, New Threats, New Opportunities

New Technologies, New Threats, New Opportunities

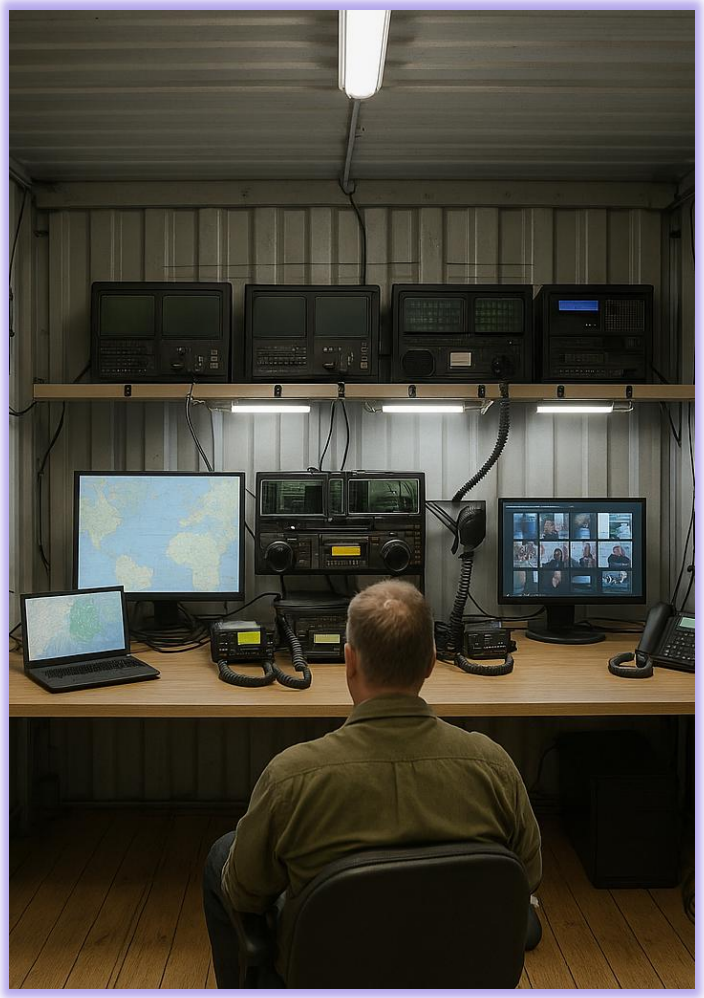


Artificial Intelligence and Machine Learning

- Offensive Applications
  - Autonomous Attack Systems
  - Behavioral Pattern Recognition
  - Deception Operations
- Defensive Applications
  - Anomaly Detection
  - Predictive Maintenance
  - Autonomous Defensive Maneuvers

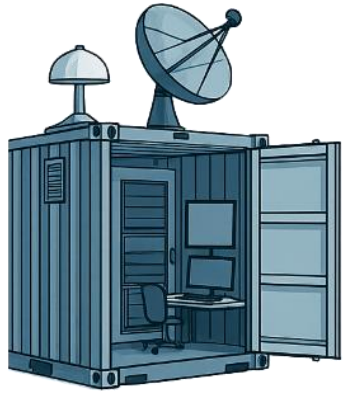
Boundary Reconnaissance Information Center (BRIC) – Modular Edge Intelligence Hub

- Rugged, Modular Deployment: ISO container system for austere, disconnected, and denied environments.
- AI-Driven Intelligence Processing: Edge analytics for ISR, cyber operations, and unmanned coordination.
- Resilient Multi-Network Communications: Dual-satellite, self-healing mesh, and active cyber defense.
- Autonomous Infrastructure: Smart power, climate control, and secure classified data management.
- Dynamic Mission Adaptation: Modular payloads and networking tailored to evolving operational needs.
- Self-Healing Security Framework: Integrated tamper response, zero-trust segmentation, and adaptive cyber defense.



BRIC: Redefining Resilient, Autonomous Operations at the Tactical Edge

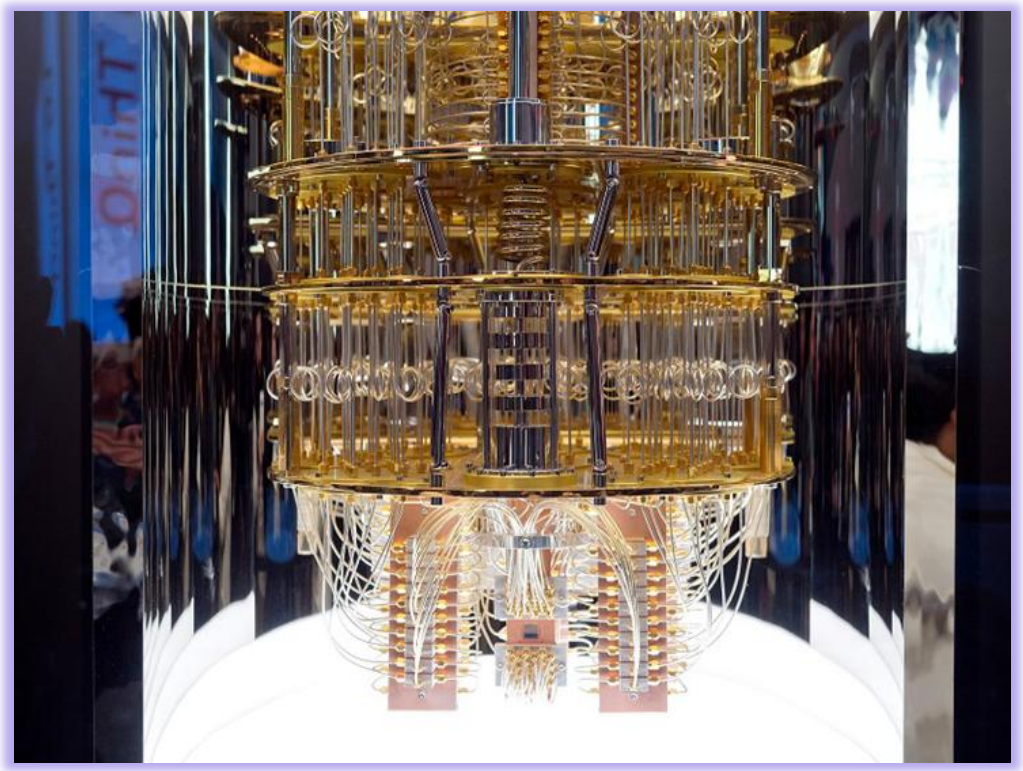
- Assured Mission Continuity
  - Operates autonomously through infrastructure, comms, or cyber degradation.
- Accelerated Decision Superiority
  - Provides real-time threat classification, sensor fusion, and operator recommendations at the point of need.
- Rapid Theater Integration:
  - Native compliance with Army Interoperability Profiles (IOP) and JADC2 frameworks.
- Low-Overhead Sustainment:
  - Smart diagnostics, hot-swap modules, and minimized logistics footprint for distributed operations.
- Scalable Across Domains:
  - From tactical ISR overwatch to theater-level cyber terrain defense.
- Strategic Endorsement:
  - Bipartisan U.S. congressional support and COCOM interest for accelerated prototyping and deployment.



New Technologies, New Threats, New Opportunities

Quantum Computing Impacts

- Cryptographic Vulnerabilities
  - Breaking Current Encryption
  - Command Authentication Risk from authentication forgery
  - Data Exposure
- Quantum Security Opportunities
  - Quantum Key Distribution (QKD)
  - Post-Quantum Cryptography
  - Quantum Random Number Generation



Appy What You Learned Today

Next week you should:

- Listen how often you hear someone talking about space
- Identify all your daily activities that require satellites

In the first 3 Months following this presentation:

- Implement a more thorough vulnerability assessment process
- Expanded threat intelligence capabilities

In the first 6 months you should:

- Approach to deeper security architecture reviews
- Identify opportunities to implement AI/ML and quantum-resistant encryption methods

RSAC 2025 Conference

Many Voices.
One Community.

H. Barbara Grofe
Spartan Corp
1-307-631-5840
hbgrofe@spartancorp.us